

533 Rec'd PCT/PTO 14 SEP 2000

FORM PTO-1390 REV. 5-93		US DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE	ATTORNEYS DOCKET NUMBER <b>P00,0637</b>
<b>TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371</b>			U.S. APPLICATION NO. (if known, see 37 CFR 1.5) <b>09/646167</b>
INTERNATIONAL APPLICATION NO. <b>PCT/DE99/00415</b>	INTERNATIONAL FILING DATE <b>16 February 1999</b>	PRIORITY DATE CLAIMED <b>16 March 1998</b>	
TITLE OF INVENTION <b>AUTHENTICATION OF KEY DEVICES</b>			
APPLICANT(S) FOR DO/EO/US <b>ANTON ENTERROTTACHER ET AL.</b>			
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:			
1. <input checked="" type="checkbox"/> This is a <b>FIRST</b> submission of items concerning a filing under 35 U.S.C. 371. 2. <input type="checkbox"/> This is a <b>SECOND</b> or <b>SUBSEQUENT</b> submission of items concerning a filing under 35 U.S.C. 371. 3. <input checked="" type="checkbox"/> This express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay. 4. <input checked="" type="checkbox"/> A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date. 5. <input checked="" type="checkbox"/> A copy of International Application as filed (35 U.S.C. 371(c)(2)). a. <input checked="" type="checkbox"/> is transmitted herewith (required only if not transmitted by the International Bureau). b. <input type="checkbox"/> has been transmitted by the International Bureau. c. <input type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US) 6. <input checked="" type="checkbox"/> A translation of the International Application into English (35 U.S.C. 371(c)(2)). 7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. §371(c)(3)) a. <input type="checkbox"/> are transmitted herewith (required only if not transmitted by the International Bureau). b. <input type="checkbox"/> have been transmitted by the International Bureau. c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired. d. <input checked="" type="checkbox"/> have not been made and will not be made. 8. <input type="checkbox"/> A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)). 9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). 10. <input checked="" type="checkbox"/> A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)). <b>Items 11. to 16. below concern other document(s) or information included:</b> 11. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 C.F.R. 1.97 and 1.98; (PTO 1449, Prior Art, Search Report). 12. <input checked="" type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included. <b>(SEE ATTACHED ENVELOPE)</b> 13. <input checked="" type="checkbox"/> Amendment "A" prior to action. <input type="checkbox"/> A SECOND or SUBSEQUENT preliminary amendment. 14. <input type="checkbox"/> A substitute specification. 15. <input checked="" type="checkbox"/> Change of Address of Applicants' Representative. 16. <input checked="" type="checkbox"/> Other items or information: a. <input checked="" type="checkbox"/> Abstract Replacement Page 7 attached to Amendment "A". b. <input checked="" type="checkbox"/> Appointment of Associate Power of Attorney. c. <input checked="" type="checkbox"/> EXPRESS MAIL # EJ077700888US dated September 14, 2000			

09/646167

PCT/DE99/00415

P00,0637

430 Rec'd PCT/PTO 14 SEP 2000

17. ☒ The following fees are submitted:**BASIC NATIONAL FEE (37 C.F.R. 1.492(a)(1)-(5):**

Search Report has been prepared by the EPO or JPO ..... \$840.00

International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) . . \$670.00

No international preliminary examination fee paid to USPTO (37 C.F.R. 1.482) but  
international search fee paid to USPTO (37 C.F.R. 1.445(a)(2)) ..... \$760.00Neither international preliminary examination fee (37 C.F.R. 1.482) nor international  
search fee (37 C.F.R. 1.445(a)(2)) paid to USPTO ..... \$970.00International preliminary examination fee paid to USPTO (37 C.F.R. 1.482) and all  
claims satisfied provisions of PCT Article 33(2)-(4) ..... \$ 96.00**ENTER APPROPRIATE BASIC FEE AMOUNT =**

CALCULATIONS

PTO USE ONLY

\$ 840.00

Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months  
from the earliest claimed priority date (37 C.F.R. 1.492(e)).

\$

Claims

Number Filed

Number  
Extra

Rate

Total Claims

04

- 20 =

0

X \$ 18.00

\$

Independent Claims

01

- 3 =

0

X \$ 78.00

\$

Multiple Dependent Claims

\$260.00 +

\$

**TOTAL OF ABOVE CALCULATIONS =**

\$ 840.00

Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must  
also be filed. (Note 37 C.F.R. 1.9, 1.27, 1.28)

\$

**SUBTOTAL =**

\$ 840.00

Processing fee of \$130.00 for furnishing the English translation later than ☐ 20 ☐ 30 months  
from the earliest claimed priority date (37 CFR 1.492(f)).

\$

**TOTAL NATIONAL FEE =**

\$ 840.00

Fee for recording the enclosed assignment (37 C.F.R. 1.21(h)). The assignment must be  
accompanied by an appropriate cover sheet (37 C.F.R. 3.28, 3.31). \$40.00 per property

\$

**TOTAL FEES ENCLOSED =**

\$ 840.00

Amount to be  
refunded

\$

charged

\$

a. ☒ A check in the amount of \$ 840.00 to cover the above fees is enclosed.b. ☐ Please charge my Deposit Account No. \_\_\_\_\_ in the amount of \$ \_\_\_\_\_ to cover the above fees.  
A duplicate copy of this sheet is enclosed.c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any  
overpayment to Deposit Account No. 501519. A duplicate copy of this sheet is enclosed.**NOTE:** Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (37 C.F.R. 1.137(a) or (b)) must be  
filed and granted to restore the application to pending status.**SEND ALL CORRESPONDENCE TO:**SCHIFF HARDIN & WAITE  
PATENT DEPARTMENT  
6600 Sears Tower  
Chicago, Illinois 60606-6473

SIGNATURE

Mark Bergner

NAME

45,877

Registration Number

09/646167

430 Rec'd PCT/PTO

14 SEP 2000

**CERTIFICATE OF MAILING BY EXPRESS MAIL**

**Express Mail Mailing Label Number EJ 077700888US**

**Date of Deposit: September 14, 2000**

I hereby certify that this correspondence is being deposited with the United States Postal "Express Mail Post Office to Addressee" service under 37 CFR 1.10(c) on the date indicated above and is addressed to:

**BOX PCT  
Assistant Commissioner for Patents  
Washington DC 20231**

**Case Number: P00,0637  
Applicant(s): Anton Enterrottacher et al.**

**International Application No. PCT/DE99/00415  
International Filing Date 16 February 1999  
Priority Date Claimed 16 March 1998**

**Title: AUTHENTICATION OF KEY DEVICES**

**Enclosed are the following documents:**

International application as filed;  
English Translation;

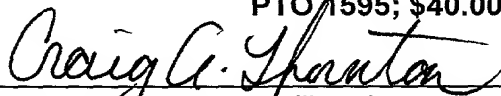
Executed Declaration;  
Change of Address form for Applicants' Representative;

PTO 1390 in duplicate;  
Amendment "A" prior to action;  
Information Disclosure Statement; PTO 1449, Search Report, 7 References;

Appointment of Associate Power of Attorney;

Fee: \$ 840.00  
Postcard.

**(See attached envelope for Executed Assignment;  
PTO 1595; \$40.00 filing fee; Postcard)**

  
\_\_\_\_\_  
Signature of person mailing documents and fees

-1-

BOX PCT  
IN THE UNITED STATES ELECTED OFFICE  
OF THE UNITED STATES PATENT AND TRADEMARK OFFICE  
UNDER THE PATENT COOPERATION TREATY-CHAPTER II

5

**AMENDMENT "A" PRIOR TO ACTION**

APPLICANT(S): Anton Enterrottacher et al.  
ATTORNEY DOCKET NO.: P00,0637  
INTERNATIONAL APPLICATION NO: PCT/DE99/00415  
INTERNATIONAL FILING DATE: 16 February 1999

10

INVENTION: **AUTHENTICATION OF KEY DEVICES**

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

15

Applicants amend the above-identified PCT application as follows, and  
request entry of the Amendment prior to examination in the United States National  
Examination Phase.

**IN THE SPECIFICATION:**

At the top of each page, please delete "GR 98 P 1347".

**On page 1:**

20

delete lines 1-6 and insert the following:

--A METHOD FOR AUTHENTICATION OF KEY DEVICES  
BACKGROUND OF THE INVENTION

25

The invention relates to a method for authenticating key devices using an  
asymmetric encryption method in which each key device is assigned a device  
specific certificate.--;

line 13, delete ", in general,";

line 17, delete ",";

line 19, delete ","; and

line 23, delete ",".

30

**On page 2:**

line 2, replace "literature" with --above-mentioned--;

line 3, delete "mentioned initially";

001160 6349300

line 5, delete “,”;

after line 15, as a separate line before line 16, insert the following heading:

--SUMMARY OF THE INVENTION--;

line 16, after “The” insert --present--; and replace “object of” with

5 --need for--;

line 17, replace “using” with --with--;

delete lines 20-21 and insert the following:

--This need is met by an aspect of the present invention including a method  
for authenticating key devices using an asymmetric encryption method in which  
10 each key device is assigned a device-specific certificate. The method includes  
assigning each key device a group-specific signature key and also a group-specific  
signature of the device specific certificate. Furthermore, a group is comprised of  
a limited total number of key devices.

According to another aspect of the present invention, the group-specific  
15 signature key and the group-specific signature are allocated to each key device  
during a first initialization.

According to yet another aspect of the present invention, the steps of  
assigning the group-specific signature key and the group-specific signature of the  
device-specific certificate to an associated specific group is determined by  
20 comparing each key device with a stored list of approved key devices.

According to a further aspect of the present invention, a link is established  
between at least two key devices. A corresponding device-specific certificate and  
a corresponding device-specific signature key is transmitted from one of the key  
devices to another one of the key devices. Another one of the key devices then  
25 verifies authenticity of the corresponding device-specific certificate using the  
corresponding device-specific signature key according to the relationship:

$$D(S(Z(A)), pAD) = D(E(Z(A)), sAD), pAD = Z(A)$$

where D represents a decryption function, S(Z(A)) represents signature of  
the corresponding device-specific certificate, E(Z(A)) represents an encryption  
30 function of the corresponding device-specific certificate, pAD represents a  
signature key of an administrator, sAD represents a secret key of the administrator  
and Z(A) represent the corresponding device-specific certificate.

Additional advantages and novel features of the present invention will be set forth, in part, in the description that follows and, in part, will become apparent to those skilled in the art upon examination of the following or may be learned by practice of the invention. The advantages of the invention may be realized and  
5 attained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS--;

lines 23-24, replace "an exemplary embodiment" with --preferred embodiments--; and

10 line 25, before ":" insert --that follows--.

**On page 3:**

line 6, after "The" insert --present--;

replace line 11 with the following: --any other device and wherein the devices involved are--;

15 line 14, replace "per se, in practice" with --in the art--;

line 15, replace "this" with --the corresponding--;

line 18, after "the" insert --present--;

line 22, delete ","; and after "be" (second occurrence) insert --stored--;

line 23, replace ", for example" with --such as--;

20 line 24, after "card" insert --, for example--; replace "Such a" with Each of the--; and replace "group" with --groups--;

line 29, replace "per se" with --in the art--;

line 31, replace ":" with --according to the relationship--; and

after "sAD)" insert --.--.

25 **On page 4:**

line 1, delete ",";

line 2, replace ", in" with --within--;

replace line 3 with --The secret key (sAD, sX) and the public key--;

line 4, replace "pAD, pX" with --(pAD, pX)--;

30 line 5, replace "which" with --that--;

line 10, replace "a refinement" with --an embodiment--;

line 15, replace "him" with --the administrator--;

line 18, replace ", that is to say" with --(i.e.,--;

line 19, after "devices" insert --)--;

line 20, delete ",";

line 22, replace ", that is to say" with --(i.e.,--;

line 23, replace "," with --)--;

5 line 24, replace ", that is to say" with --(i.e.,--;

line 25, replace ":" with --) according to the relationship:--;

line 26, replace "D (E (Z (A), sAD), pAD) = Z (A)" with --  
D (E (Z (A) ), sAD), pAD) = Z (A).--;

line 29, replace "A" with --Hence,--; and

10 line 31, replace "can thus" with --, thus, can--.

**On page 5:**

line 2, delete ",";

line 7, delete ","; and

after line 8, insert the following paragraph:

15 --While this invention has been described in connection with what are  
presently considered to be the most practical and preferred embodiments, it is to  
be understood that the invention is not limited to the disclosed embodiments, but,  
on the contrary, is intended to cover various modifications and equivalent  
arrangements included within the spirit and scope of the appended claims.--

20 **IN THE CLAIMS:**

On page 6, replace "Patent Claims" with --What is claimed is:--.

**Cancel claims 1-3 without prejudice or disclaimer.**

**Please add new claims 4-7 as follows.**

25 4. A method for authenticating key devices using an asymmetric encryption  
method in which each key device is assigned a device-specific certificate, the  
method comprising the steps of:

assigning each key device a group-specific signature key; and

assigning each key device a group-specific signature of the device-specific  
certificate;

30 wherein a group is comprised of a limited total number of key devices.

5. The method according to claim 4, wherein the group-specific signature key and the group-specific signature of the device-specific certificate are allocated to each key device during a first initialization.

5 6. The method according to claim 4, wherein the steps of assigning the group-specific signature key and the group-specific signature of the device-specific certificate to an associated specific group are each determined by comparing each key device with a stored list of approved key devices.

7. The method according to claim 4, further comprising the steps of:  
establishing a link between at least two key devices;  
10 transmitting a corresponding device-specific certificate and a corresponding device-specific signature key from one of the key devices to another one of the key devices, the another one of the key devices verifying authenticity of the corresponding device-specific certificate using the corresponding device-specific signature key according to the relationship:

15 
$$D(S(Z(A)), pAD) = D(E(Z(A)), sAD), pAD = Z(A)$$

where D represents a decryption function, S(Z(A)) represents signature of the corresponding device-specific certificate, E(Z(A)) represents an encryption function of the corresponding device-specific certificate, pAD represents a signature key of an administrator, sAD represents a secret key of the administrator, and Z(A) represents the corresponding device-specific certificate.  
20

**IN THE ABSTRACT:**

Delete original page 7 and replace the Abstract with Replacement Page 7, which is provided on a separate sheet attached to the amendment.



**REMARKS**

5 The present amendment makes editorial changes to the specification, drawings, claims and Abstract in order to conform the United States Patent Practice. Additionally, the Applicants include herewith a copy of the new Abstract on a separate page. None of the changes in the claims is intended as a surrender of any of the subject matter within the scope of the original claim language since, as noted above, all of these changes have been made solely to bring the claims into conformity with the requirements of 35 U.S.C. §112, second paragraph.

Early consideration of the application is respectfully requested.

10 Respectfully submitted,

15  (Reg. No. 45,877)  
Mark Bergner  
SCHIFF HARDIN & WAITE  
PATENT DEPARTMENT  
6600 Sears Tower  
Chicago, Illinois 60606-6473  
(312) 258-5779  
ATTORNEY FOR APPLICANT

## 5

A method for authentication of key devices using an asymmetric encryption method, in which the key device is assigned a device-specific certificate. According to the invention, each key device is assigned a group-specific signature key and a group-specific signature of the certificate, with a group being composed of a limited total number of key devices.

## Description

## Authentication of key devices

5           The invention relates to a method as claimed in  
the precharacterizing clause of patent claim 1.

Such a method is described in principle in the book by W. Fumy and H.P. Rieß: Kryptographie, Entwurf und Analyse symmetrischer Kryptosysteme [Cryptography, Design and Analysis of Symmetrical Cryptosystems] R. Oldenbourg Verlag, Munich Vienna, 1988, ISBN 3-486-20868-3.

When voice or, in general, data are transmitted in encrypted form, both communication partners must have a joint secret, the keyword. This keyword is unknown to a potential eavesdropper or enemy. One option for this is an asymmetric encryption method, in which random numbers are interchanged between the communication partners, and are used to form joint keywords.

With this method, it is impossible to determine whether the encrypted link is being set up with the desired communication partner, or with an enemy.

25 Cryptographic methods may be used not only for secrecy, but also for authentication of messages. The encryption of a message using a keyword also, in principle, includes its authenticity, since an enemy cannot produce the clear text of the message without knowledge of the keyword.

30           In an asymmetric cryptosystem, the keyword used for encryption of a message is different to that used for decryption. Such a system, with a public and a private key, is also referred to as a public key system. The best known example of the

public key system is the so-called RSA method, whose principles are likewise described in the literature reference mentioned initially.

At first glance, the system of key distribution is largely solved when using asymmetric cryptosystems, since the public keys can be interchanged without any problems via insecure data channels. However, this is true only provided that eavesdropping is regarded as the only risk to a communications link. However, in most cases, it is also necessary to take account of the possibility of active attacks, in addition to passive eavesdropping attempts. In this case, an active enemy introduces himself into the data link between two subscribers. Such an attack can be identified only when authentication measures are used.

The invention is based on the object of specifying a method using which it is possible to authenticate the key devices involved in data interchange.

This object is achieved according to the invention by the features specified in patent claim 1.

The invention will be described in the following text with reference to an exemplary embodiment. The following abbreviations are used in the description:

E	Encryption
D	Decryption
A, B, X	Subscribers
AD	Administrator
p	Public key
s	Secret key
pAD	Signature key, corresponds to the public key p of the administrator AD

Z Certificate, corresponds to the public key p,  
to the name and further details of a  
subscriber X

S Signature

5 S(Z) Signature of the certificate Z

The invention is based on a cryptomethod in  
which all the encryption devices are equipped with a  
joint public key. This public key pAD is allocated by a  
trustworthy entity, a so-called administrator AD. In  
10 principle, this allows any device to communicate with  
any other, with the devices involved being  
authenticated.

Each key device is individually assigned a  
certificate Z in a manner known per se, in practice in  
15 the form of a name for this device. In addition, when  
using the public key system, the certificate Z contains  
the public key pX for the subscriber or user X.

According to the invention, user groups are  
formed whose devices are equipped with a joint,  
20 group-specific signature key pAD. This signature key  
pAD is the public key pAD of the administrator AD. It  
may be stored in the device itself, or may be in the  
form of other storage means, for example on a smart  
card. Such a user group has a limited number of  
25 subscribers. This limits the dissemination of the  
signature key pAD.

The administrator AD can produce a signature  
S(Z(X)) for a certificate Z(X) for a user X in a manner  
known per se. In this case, the certificate Z(X) is  
30 encrypted using the secret key sAD of the administrator  
AD.

$$S(Z(X)) = E(Z(X), sAD)$$

This signature  $S(Z(X))$  is likewise stored, in fixed or mobile form, in the key device of the user X.

The secret key and the public key  $sAD$ ,  $sX$  and  $pAD$ ,  $pX$  of the administrator AD and of the subscribers X are part of the public key system which is implemented, for example, using the RSA algorithms.

The group-specific signature key  $pAD$  and the subscriber-specific or device-specific signature  $S(Z(X))$  are, for example, loaded in the key device on first initialization, in a refinement of the invention. In addition, the associated certificate  $Z(X)$  is stored in the key device. These data may also be distributed to the appropriate subscriber on a smart card. Personal contact with the administrator AD, or at least a secure transmission channel to him, is required for these procedures.

For secure communication, a link is set up between the subscribers A and B, that is to say between the associated key devices. The subscriber A transmits the certificate  $Z(A)$ , and the signature  $S(Z(A))$  to the subscriber B. The subscriber B can use the signature key  $pAD$ , that is to say the public key  $p$  of the administrator AD, to verify the authenticity of the certificate  $Z(A)$ , that is to say the authenticity of the subscriber A:

$$D(S(Z(A)), pAD) = D(E(Z(A), sAD), pAD) = Z(A)$$

The subscriber A checks the subscriber B in an analogous manner.

A potential attacker is external to the group, has no signature  $S$  assigned by the administrator AD, and can thus not set up a link to any subscriber in this group.

- 5 -

In the event of theft, the corresponding devices are excluded from the user group, so that they cannot be used by an attacker. To do this, in one possible refinement of the invention, a list of approved subscribers or key devices is stored in the key device. The identities of the possible key devices may be stored, with an appropriate security question being integrated in the process of setting up a link.





## Abstract

## Authentication of key devices

5           The invention relates to a method for authentication of key devices using an asymmetric encryption method, in which the key device is assigned a device-specific certificate (Z). According to the invention, each key device is assigned a group-specific signature key (pAD) and a group-specific signature (S(Z)) of the certificate (Z), with a group being composed of a limited total number of key devices.

# Declaration and Power of Attorney For Patent Application

## *Erklärung Für Patentanmeldungen Mit Vollmacht*

### German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

#### Authentifizierung von Schlüsselgeräten

deren Beschreibung

(zutreffendes ankreuzen)

☒ hier beigefügt ist.

☐ am \_\_\_\_\_ als

PCT internationale Anmeldung

PCT Anmeldungsnummer \_\_\_\_\_

eingereicht wurde und am \_\_\_\_\_

abgeändert wurde (falls tatsächlich abgeändert).

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

the specification of which

(check one)

☐ is attached hereto.

☐ was filed on \_\_\_\_\_ as

PCT international application

PCT Application No. \_\_\_\_\_

and was amended on \_\_\_\_\_  
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

# German Language Declaration

Prior foreign applications  
Priorität beansprucht

Priority Claimed

19811318.8      Germany      16. März 1998  
(Number)      (Country)      (Day Month Year Filed)  
(Nummer)      (Land)      (Tag Monat Jahr eingereicht)

☒      ☐  
Yes      No  
Ja      Nein

\_\_\_\_\_  
(Number)      (Country)      (Day Month Year Filed)  
(Nummer)      (Land)      (Tag Monat Jahr eingereicht)

☐      ☐  
Yes      No  
Ja      Nein

\_\_\_\_\_  
(Number)      (Country)      (Day Month Year Filed)  
(Nummer)      (Land)      (Tag Monat Jahr eingereicht)

☐      ☐  
Yes      No  
Ja      Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemäss Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

\_\_\_\_\_  
(Application Serial No.)  
(Anmeldeseriennummer)

\_\_\_\_\_  
(Filing Date)  
(Anmeldedatum)

\_\_\_\_\_  
(Status)  
(patentiert, anhängig,  
aufgegeben)

\_\_\_\_\_  
(Status)  
(patented, pending,  
abandoned)

\_\_\_\_\_  
(Application Serial No.)  
(Anmeldeseriennummer)

\_\_\_\_\_  
(Filing Date)  
(Anmeldedatum)

\_\_\_\_\_  
(Status)  
(patentiert, anhängig,  
aufgeben)

\_\_\_\_\_  
(Status)  
(patented, pending,  
abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefängnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

## German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: (Name und Registrationsnummer anführen)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. (list name and registration number)

And I hereby appoint

Messrs. John D. Simpson (Registration No. 19,842) Lewis T. Steadman (17,074), William C. Stueber (16,453), P. Phillips Connor (19,259), Dennis A. Gross (24,410), Marvin Moody (16,549), Steven H. Noll (28,982), Brett A. Valiquet (27,841), Thomas I. Ross (29,275), Kevin W. Guynn (29,927), Edward A. Lehmann (22,312), James D. Hobart (24,149), Robert M. Barrett (30,142), James Van Santen (16,584), J. Arthur Gross (13,615), Richard J. Schwarz (13,472) and Melvin A. Robinson (31,870), David R. Metzger (32,919), John R. Garrett (27,888) all members of the firm of Hill, Steadman & Simpson, A Professional Corporation.

Telefongespräche bitte richten an:  
(Name und Telefonnummer)

Direct Telephone Calls to: (name and telephone number)

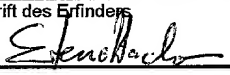
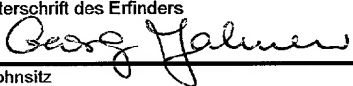
312/876-0200

Ext. \_\_\_\_\_

Postanschrift:

Send Correspondence to:

**HILL, STEADMAN & SIMPSON**  
A Professional Corporation  
85th Floor Sears Tower, Chicago, Illinois 60606

Voller Name des einzigen oder ursprünglichen Erfinders:		Full name of sole or first inventor:	
<b>ENTERROTTACHER, Anton</b>			
Unterschrift des Erfinders	Datum	Inventor's signature	Date
	3.2.99		
Wohnsitz		Residence	
<b>D-80639 München Germany</b>		DEX	
Staatsangehörigkeit		Citizenship	
<b>Bundesrepublik Deutschland</b>			
Postanschrift		Post Office Address	
<b>Gassnerstr. 9</b>			
<b>D-80639 München</b>			
<b>Bundesrepublik Deutschland</b>			
Voller Name des zweiten Miterfinders (falls zutreffend):		Full name of second joint inventor, if any:	
<b>JAHNEN, Georg</b>			
Unterschrift des Erfinders	Datum	Second Inventor's signature	Date
	3.2.99		
Wohnsitz		Residence	
<b>D-85716 Unterschleissheim Germany</b>		DEX	
Staatsangehörigkeit		Citizenship	
<b>Bundesrepublik Deutschland</b>			
Postanschrift		Post Office Address	
<b>Raiffeisenstr. 56</b>			
<b>D-85716 Unterschleissheim</b>			
<b>Bundesrepublik Deutschland</b>			

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).

COPY TO: 2-80

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT(S): Anton Enterrottacher et al.  
 ATTORNEY DOCKET NO.: P00,0637  
 INTERNATIONAL APPLICATION NO: PCT/DE99/00415  
 INTERNATIONAL FILING DATE: 16 February 1999  
 INVENTION: **AUTHENTICATION OF KEY DEVICES**


Assistant Commissioner for Patents,  
 Washington, D.C. 20231

APPOINTMENT OF ASSOCIATE POWER OF ATTORNEY

Sir:

I am an attorney designated on the Power of Attorney for the above-referenced application. I hereby appoint Mark Bergner (Reg. No. 45,877) as an associate attorney, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Submitted by,

 (Reg. No. 31,870)  
 Melvin A. Robinson  
 SCHIFF HARDIN & WAITE  
 PATENT DEPARTMENT  
 6600 Sears Tower  
 Chicago, Illinois 60606-6473  
 (312) 258-5785  
 Attorney for Applicant(s)

Date: September 14, 2000

004607 2585785

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CHANGE OF ADDRESS OF APPLICANTS' REPRESENTATIVE

APPLICANT(S): Anton Enterrottacher et al.

ATTORNEY DOCKET NO.: P00,0637

INTERNATIONAL APPLICATION NO: PCT/DE99/00415

INTERNATIONAL FILING DATE: 16 February 1999

INVENTION: **AUTHENTICATION OF KEY DEVICES**

Assistant Commissioner for Patents,  
Washington, D.C. 20231

S I R:

Members of the firm of Hill & Simpson designated on the original Power of Attorney have merged into the firm of Schiff Hardin & Waite. All future correspondence for the above-referenced application therefore should be sent to the following address:

**SCHIFF HARDIN & WAITE**  
**Patent Department**  
**6600 Sears Tower**  
**233 South Wacker Drive**  
**Chicago, Illinois 60606-6473**

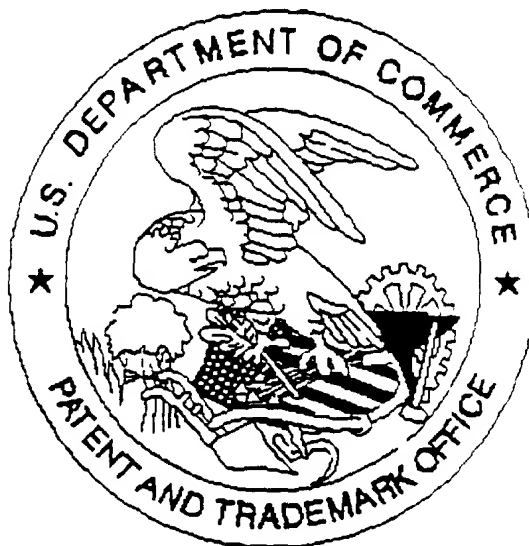
Submitted by,

*Mark Bergner*

(Reg. No. 45,877)

Mark Bergner  
SCHIFF HARDIN & WAITE  
Patent Department  
6600 Sears Tower  
Chicago, Illinois 60606-6473  
Telephone: (312) 258-5779  
Attorneys for Applicants

United States Patent & Trademark Office  
Office of Initial Patent Examination -- Scanning Division



SCANNED, # 24

Application deficiencies were found during scanning:

☐ Page(s) 1 of Drawing were not present  
for scanning. (Document title)

☐ Page(s) \_\_\_\_\_ of \_\_\_\_\_ were not present  
for scanning. (Document title)

☐ Scanned copy is best available.